On eigenvectors of the discrete Fourier transform over finite Gaussian fields

A.N. Karkishchenko[1], **V.B. Mnukhin**[1]

[1] Southern Federal University, 105/42, Bolshaya Sadovaya, Rostov-na-Donu, Russia, 344006

Abstract. The problem of furnishing orthogonal systems of eigenvectors for the discrete Fourier transform (DFT) is fundamental to image processing with applications in image compression and digital watermarking. This paper studies some properties of such systems for DFT over finite fields that may be considered as "finite complex planes". Some applications for multiuser communication schemes are also considered.

Keywords: eigenvectors, discrete Fourier transform, finite fields, Gaussian fields, image compression.

1. Introduction

The problem of investigating the discrete Fourier transform (DFT) and, especially its eigenstructure, is one of the classical problems of mathematics [1]. Currently such generalizations of DFT as the Hartley transform, the wavelet transform and trigonometric transforms are under intensive study and have numerous applications in digital multiplexing systems design, multiple access systems, error-correcting coding, cryptography, ets [2, 3, 4].

Also transforms in finite fields have been intensively studied and applied after Pollard defined the fast Fourier transform in a finite field [5]. In digital signal and image processing these transforms are attractive because they avoid floating point operations and rounding errors. As a result, in comparison with real-valued mathematical tools, faster hardware implementations could be designed [6, 7, 8, 9].

In spite of the fact that eigenstructure of a number of such transforms is in general known [10], a lot of questions are still open. Partly it is related with large dimensions of eigenspaces and with the lack of any canonical bases in it. So the problem of finding systems of eigenvectors with any nice special properties is currently actual [11, 12, 13].

Encouraged by the above presented aspects, this paper has the main purpose of introducing a new system of eigenvectors for the discrete Fourier transform over "finite complex fields", called Gaussian fields. Such eigenvectors have a very simple structure related with subgroups of the multiplicative group of the field and are potentially useful in multiuser communication schemes [2, 4]. and image compression.

The paper is organized as follows. After the introducing finite Gaussian fields in the next section and the discrete Fourier transform in Section 3, eigenvalues of such *cyclic* FT are studied in Section 4, where the general form of eigenvectors is shown. Then in Section 5 we introduce subgroup eigenspaces and construct its bases. The paper closes with some concluding remarks in Section 6.

2. Finite Fields of Gaussian Integers

Let $\mathbb{Z}$ and $\mathbb{C}$ be the ring of integers and the complex field respectively, let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ be a residue class ring modulo an integer $n \geq 2$, and let $\mathbb{GF}(p^m)$ be a Galois field with p^m elements, where p is a prime and $m > 0$ is an integer.

In number theory [14, Ch. 1.4] a *Gaussian integer* is a complex number $z = a + bi \in \mathbb{C}$ whose real and imaginary parts are both integers. Note that within the complex plane the Gaussian integers may be seen to constitute a square lattice.

Gaussian integers, with ordinary addition and multiplication of complex numbers, form the subring $\mathbb{Z}[i]$ in the field $\mathbb{C}$. Unfortunately, lack of division in such rings significantly restricts its applicability to image processing problems [15, 16, 17, 18]. So it is natural to look for finite fields, whose properties would be in some respect similar to properties of $\mathbb{C}$. Note, that if $p = 4k+3$ is a prime, then the polynomial $x^2 + 1$ is irreducible over $\mathbb{Z}_p$. As an immediate corollary, the next definition follows.

Definition 1. Let $p \geq 3$ be a prime number such that $p \equiv 3 \pmod 4$. Then the finite field

$$\mathbb{C}(p) \stackrel{\text{def}}{=\!=} \mathbb{Z}_p[x]/(x^2 + 1) \simeq \mathbb{GF}(p^2)$$

will be called *Gaussian field*. Elements of $\mathbb{C}(p)$ will be called *discrete Gaussian numbers*.

Thus, Gaussian fields have p^2 elements, where

$$p = 3,\ 7,\ 11,\ 19,\ 23,\ 31,\ 43,\ 47,\ 59,\ 67,\ 71,\ 79,\ 83,\ 103,\ \ldots\ .$$

In particular, there are 87 fields $\mathbb{C}(p)$ for $3 \leq p < 1000$. Elements of Gaussian fields are of the form $z = a + bi$, where $a, b \in \mathbb{Z}_p$ and i denotes the class of residues of x, so that $i^2 + 1 = 0$. The multiplication and addition in $\mathbb{C}(p)$ is straightforward, just as notions of the *conjugate* to z number $z^* = a - bi \in \mathbb{C}(p)$ and the *norm* $N(z) = zz^* = a^2 + b^2 \in \mathbb{Z}_p$. (Note that in $\mathbb{C}(p)$ the concept of modulus $|z| = \sqrt{N(z)}$ is not defined.) It is easy to show that $N(z_1 z_2) = N(z_1)N(z_2)$ and $N(z) = 0 \ \Leftrightarrow \ z = 0$.

3. Fourier transform over Gaussian fields

Let $\mathbb{C}(p)$ be any Gaussian field of a characteristic $p = 4k + 3$ Note that since $\mathbb{C}(p)$ is finite, its multiplicative group $\mathbb{C}^*(p) = \mathbb{C}(p) \setminus \{0\}$ is cyclic and generated by a primitive element g. For example, $g = 2 + 7i$ and $p = 1 + 19i$ are primitive in $\mathbb{C}^*(71)$ and $g = 1 + 5i$ is primitive for $p = 251$.

Let $K = |G| = p^2 - 1$ and let $\big(f_0, f_1, \ldots, f_{K-1}\big)$ be a vector of length K with $f_s \in \mathbb{C}(p)$. Note that such vectors are in natural correspondence with functions $f(z) : \mathbb{C}(p) \to \mathbb{C}(p)$ such that $f(g^s) = f_s$, and from now on we will identify functions with vectors (f_s).

There is another way to consider functions on $\mathbb{C}(p)$. Let $\mathbb{C}(p)[G] \simeq \mathbb{C}(p)[X]/(X^K - 1)$ be the group algebra of the cyclic group G over the field $\mathbb{C}(p)$. Its elements may be considered as "polynomials" in the indeterminate X,

$$q_f(X) = f_0 + f_1 X + f_2 X^2 + \cdots + f_{K-1} X^{K-1} \in \mathbb{C}(p)[X]/(X^K - 1)\ ,$$

where the vector of coefficients $f_s \in \mathbb{C}(p)$ defines a function f. Thus, we have the bijection

$$f \longleftrightarrow q_f(X)$$

and we will call $q_f(X)$ the *polinomial* representation of f.

Definition 2. Let $\mathbb{C}(p)$ be a Gaussian field and let g be any generator of its multiplicative group. Let $f(z) : \mathbb{C}(p) \to \mathbb{C}(p)$ be a function and let (f_k) be the vector of its values, $f_k = f(g^k)$.

The pair of mutually inverse transforms $\mathcal{F}_g[f] = F$ and $\mathcal{F}_g^{-1}[F] = f$, given by

$$F_w = -\sum_{k=0}^{K-1} f_k g^{kw}, \qquad f_k = \sum_{w=0}^{K-1} F_w g^{-kw} .$$

will be called *cylic Fourier transform* (CFT briefly) and its inverse respectively. It can be also defined in symmetrized form by

$$F_w = i\sum_{k=0}^{K-1} f_k g^{kw}, \qquad f_k = i\sum_{w=0}^{K-1} F_w g^{-kw} .$$

Thus, the vector (F_w) is the left product of (f_k) by the Vandermonde matrix

$$U_g = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & g & g^2 & g^3 & \dots & g^{K-1} \\ 1 & g^2 & g^4 & g^6 & \dots & g^{2(K-1)} \\ 1 & g^3 & g^6 & g^9 & \dots & g^{3(K-1)} \\ \dots & \dots\dots & \dots\dots & \dots\dots & \dots & \dots\dots\dots \\ 1 & g^{K-1} & g^{2(K-1)} & g^{3(K-1)} & \dots & g^{(K-1)(K-1)} \end{pmatrix}.$$

In particular, for $p = 3$ and $K = 8$ we have $g^2 = i$, $g^4 = -1$ and $g^7 = -ig = g^{-1}$, so that

$$U_g = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & g & i & ig & -1 & -g & -i & -ig \\ 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & ig & -i & g & -1 & -ig & i & -g \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -g & i & -ig & -1 & g & -i & ig \\ 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & -ig & -i & -g & -1 & ig & i & g \end{pmatrix}$$

Note that if h is another generator for G, then $h = g^s$, then $\gcd(s, K) = 1$. Thus, in the matrices U_g and U_h the first rows and columns coincide, while other rows and columns are the same up to the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & K-1 \\ s & 2s \bmod K & 3s \bmod K & \dots & K-s \end{pmatrix}.$$

So in fact CFT does not depend on g, and we will write $\mathcal{F}[f] = F$ briefly.

4. Eigenvectors of the cyclic Fourier transform

Note that $K \equiv -1 \pmod p$. The next results are trivial:

Lemma 1. $U^2 = -\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$ *and so* $\mathcal{F}^4 = \mathcal{I}$.

Thus, eigenvalues of $\mathcal{F}$ *are* 1,i, -1, $-i$.

Lemma 2. *Eigenvalues of the transform* $\mathcal{F}^4$ *are* 1 *and* -1 *of multiplicities* $K/2-1$ *and* $K/2+1$ *respectively. The corresponding eigenspaces have the following systems of vectors as bases*

$$\phi_s^{(1)} = X^s - X^{-s} \qquad \textit{and} \qquad \phi_h^{(-1)} = X^h + X^{-h}, \qquad \textit{where } 0 < s < K/2,\ 0 \le h \le K/2.$$

Lemma 3. *Let $\mathcal{F}$ be an arbitrary linear transform with an eigenvalue λ. Let v be an eigenvector of $\mathcal{F}^2$ corresponding to the eigenvalue λ^2. Then $w = \lambda v + \mathcal{F}[v]$ is an eigenvector of $\mathcal{F}$ corresponding to λ.*

Proof. Indeed,

$$\mathcal{F}[w] = \mathcal{F}\big[\lambda v + \mathcal{F}[v]\big] = \lambda\mathcal{F}[v] + \mathcal{F}^2[v] = \lambda\mathcal{F}[v] + \lambda^2 v = \lambda\big(\lambda v + \mathcal{F}[v]\big) = \lambda w\ .$$

The next result follows from the previous lemmata immediately.

Proposition 1. *The nonzero vectors*

$$\psi_h^{(\lambda)} = \lambda\phi_h^{(\lambda^2)} + \mathcal{F}\Big[\phi_h^{(\lambda^2)}\Big], \qquad \text{where } \lambda = 1, i, -1, -i \quad \text{and} \quad 0 \le h \le K/2,$$

are eigenvectors of the Fourier transform with λ as the corresponding eigenvalue. In other words, these vectors are

$$\begin{aligned}
\psi_h^{(1)} &= \phi_h^{(1)} + \mathcal{F}\left[\phi_h^{(1)}\right] = X^h - X^{-h} + \mathcal{F}[X^h] - \mathcal{F}[X^{-h}],\\
\psi_h^{(-1)} &= -\phi_h^{(1)} + \mathcal{F}\left[\phi_h^{(1)}\right] = -X^h + X^{-h} + \mathcal{F}[X^h] - \mathcal{F}[X^{-h}],\\
\psi_h^{(i)} &= i\phi_h^{(-1)} + \mathcal{F}\left[\phi_h^{(-1)}\right] = iX^h + iX^{-h} + \mathcal{F}[X^h] + \mathcal{F}[X^{-h}],\\
\psi_h^{(-i)} &= -i\phi_h^{(-1)} + \mathcal{F}\left[\phi_h^{(-1)}\right] = -iX^h - iX^{-h} + \mathcal{F}[X^h] + \mathcal{F}[X^{-h}].
\end{aligned}$$

Evidently, not all of the vectors $\psi_h^{(\lambda)}$ are linearly independent.

5. Subgroup eigenspaces

Note that all subgroups of the cyclic group G are known: for every integer $L \le 1$ that divides $K = |G| = p^2 - 1$, there is the unique subgroup $H \le G$ of order L. Moreover, H is generated by any element $g^k \in G$ such that $\gcd(k, K) = K/L$, and there are precisely φ such generators, where φ is the totient function. If

$$K = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s},$$

then G has precisely $S(p) = (1 + \alpha_1)(1 + \alpha_2)\dots(1 + \alpha_s)$ subgroups. Note that $4|S(p)$ and $S(p) \le 2(p - 1)$, where the equality holds for $p = 3$ when $S(3) = 4 = 2(p - 1)$. The function $S(p)$ is slowly growing; in particular, $S(p) \le S(911) = 192$ for $p < 1000$.

Note that with a subgroup $H = \langle g^s \rangle \le G$ we may associate a function $\chi_H : \mathbb{C}_p \to \mathbb{C}_p$,

$$\chi_H(z) = \begin{cases} 1, & z \in H,\\ 0, & z \notin H. \end{cases}$$

Since a subgroup of G is completely determined by its order, sometimes we will refer to χ_H as $\chi_{|H|}$. As a vector, it is

$$\Big(1, \underbrace{0, 0, \dots, 0, 0}_{s-1 \text{ zeros}}, \ 1, \underbrace{0, 0, \dots, 0, 0}_{s-1 \text{ zeros}}, \ \dots\dots\Big)$$

and the corresponding polynomial is

$$1 + X^s + X^{2s} + \dots + X^{K-s}.$$

Definition 3. The subspace $\mathcal{S}_p \subset \mathbb{C}_p^K$ spanned by all the vectors ν_H will be called the *subgroup space* of G. Its dimension is $S(p)$.

It occurs that the subgroup space is closed under products, convolutions and the Fourier transform. To show it, note first that the subgroup lattice of G is distributive with the following join and meet operations: for $H, L \leq G$,

$$H \wedge L = H \cap L, \qquad \text{where} \quad |H \cap L| = \gcd(|H|, |L|),$$
$$H \vee L = \langle H, L \rangle, \qquad \text{where} \quad |H \vee L| = \frac{K}{\gcd(K/|H|\,,\, K/|L|)}.$$

Theorem 1. *The subgroup space is closed under products of functions, convolutions and the cyclic Fourier transform: for every $H, L \leq G$,*

$$\chi_H \cdot \chi_L = \chi_{H \wedge L}, \qquad \chi_H * \chi_L = |H \wedge L| \chi_{H \vee L}, \qquad \mathcal{F}\big[\chi_H\big] = |H| \chi_{G/H}\,.$$

Corollary 1. *Let $H < G$ be a subgroup of G. Then*

$$\psi_H^{(i)} = \chi_H - i|H|\chi_{G/H} \qquad \textit{and} \qquad \psi_H^{(-i)} = \chi_H + i|H|\chi_{G/H} \tag{1}$$

are eigenvectors of the cyclic Fourier transform corresponding to eigenvalues $\lambda = i$ and $\lambda = -i$ respectively.

Proof. We consider the case $\lambda = -i$ first. Note that $|G| = K = p^2 - 1 \equiv -1 \bmod p$. Hence,

$$\begin{aligned} \mathcal{F}\left[\psi_H^{(-i)}\right] &= \mathcal{F}[\chi_H] + i|H|\mathcal{F}[\chi_{G/H}] = |H|\chi_{G/H} + iK\chi_H \\ &= |H|\chi_{G/H} - i\chi_H = -i(\chi_H + i|H|\chi_{G/H}) = -i\psi_H^{(-i)}\,. \end{aligned}$$

The proof for $\psi_H^{(i)}$ is similar. ■

Note that eigenvectors corresponding to H and G/H will be the same, up to a factor. Since $|H| \cdot |G/H| = |G| = K$, we may assume in (1) that $|H| < \sqrt{K} = \sqrt{p^2 - 1} < p$. It also follows from (1) that

$$\chi_H = \frac{\psi_H^{(i)} + \psi_H^{(-i)}}{2}, \qquad \text{and} \qquad \chi_{G/H} = i\frac{\psi_H^{(i)} - \psi_H^{(-i)}}{2|H|}.$$

Now the main result of the paper can be formulated.

Theorem 2. *When restricted to the subgroup space, the cyclic Fourier transform has only two eigenvalues i and $-i$. The corresponding eigenspaces are of dimensions $S(p)/2$ each and their bases are formed by the vectors $\psi_H^{(i)}$ and $\psi_H^{(-i)}$, where $H < G$ and $|H| < p$.*

6. Conclusion

This paper proposes a new system of eigenvectors for the discrete Fourier transform over finite Gaussian fields. Such eigenvectors have a very simple structure related with subgroups of the multiplicative group of the underlying finite field. Subspace spanned by the eigenvectors are closed under products, convolutions and the DFT.

However, apart from of this work, there remain issues such as the detailed study of properties of the introduced transformations, the study of possibilities of its generalizations, as well as the details of its practical applications in multiuser communication schemes and image compression. Authors hope to return to the study of these issues in the further papers.

7. **Acknowledgements**

This research has been partially supported by the Russian Foundation for Basic Research grants no. 16-07-00648 and 17-20-02017. The authors would like to thank the anonymous referee for constructive comments and suggestions.

8. References

[1] Auslander, L. Is computing with the finite Fourier transform pure or applied mathematics? / L. Auslander, R. Tolimieri // Bull American Math Soc. — 1979. — Vol. 1. — P. 847-897.

[2] Campello de Souza, R.M. Multiuser Communication Based on the DFT Eigenstructure / R.M. Campello de Souza, H.M. de Oliveira, R.J. Cintra // arXiv:1702.01793v1 (6 Feb 2017).

[3] Lima, J.B. The eigenstructure of finite field trigonometric transforms / J.B. Lima, R.M. Campello de Souza, D. Panario // Linear Algebra and its Applications. — 2011. — Vol. 435. — P. 1956-1971.

[4] Campello de Souza, R.M. Eigensequences for multiuser communication over the real adderchannel / R.M. Campello de Souza, H.M. de Oliveira // Proc. of the International Telecommunications Symposium, Fortaleza, Brasil, 2006.

[5] Pollard, J.M. The fast Fourier transform in a finite field / J.M. Pollard // Math. Comp. — 1971. — Vol. 114. — P. 82-100.

[6] Chernov, V. M. Number-theoretic transforms in digital image processing / V.M. Chernov, A.O. Korepanov // Samara: SGAU. — 2006. — 112 p. (in Russian).

[7] Chernov, V. M. Arithmetic methods for fast algorithms for discrete orthogonal transforms development / V.M. Chernov // Moscow: FIZMATLIT. — 2007 — 264 p. (in Russian).

[8] Labunets, V. Number theoretic transforms over quadratic fields. Complex Control Systems / V. Labunets // Kiev: Institute of Cybernetics USSR. — 1982 — p. 30–37. (in Russian).

[9] Varitschenko, L. Abstract Algebraic Systems and Digital Signal Processing // L. Varitschenko, V. Labunets, M. Rakov // Kiev: Naukova Dumka. — 1986 — 248 p. (in Russian).

[10] McClellan, J.H. Eigenvalue and eigenvector decomposition of the discrete Fourier transform / J. H. McClellan, T.W. Parks // IEEE Transactions on Audio and Electroacoustics. — 1972. Vol. 20(1). — P. 6674.

[11] Berthold Horn, K.P. Interesting eigenvectors of the Fourier transform / K.P. Berthold Horn // Transactions of the Royal Society of South Africa. — 2010. — Vol. 65(2). — P. 100-106.

[12] Fendler, G. Discrete Fourier transform of prime order: Eigenvectors with small support / G. Fendler, Norbert Kaiblinger // Linear Algebra and Its Applications. — 2013. — Vol. 438(1). — P. 288-302.

[13] Santhanam, B. On discrete Gauss-Hermite functions and eigenvectors of the discrete Fourier transform / B. Santhanam , T.S. Santhanam // Signal Processing. — 2008.— Vol. 88. — P. 2738-2746.

[14] Ireland, K. A Classical Introduction to Modern Number Theory. - Springer-Verlag, 1982.

[15] Mnukhin, V.B. Transformations of Digital Images on Complex Discrete Tori / V.B. Mnukhin // Pattern Recognition and Image Analysis: Advances in Mathematical Theory and Applications. — 2014. — Vol. 24(4). — P. 552-560.

[16] Mnukhin, V.B. Digital images on a complex discrete torus / V.B. Mnukhin // Machine Learning and Data Analysis. — 2013. — Vol. 1(5). — P. 540-548.

[17] Karkishchenko, A.N. Applications of modular logarithms on complex discrete tori in problems of digital image processing / A.N. Karkishchenko, V.B. Mnukhin // Bulletin of the Rostov State University of Railway Transport — 2013. — Vol. 3. - P. 147-153.

[18] Mnukhin, V.B. Fourier-Mellin transform on a complex discrete torus / V.B. Mnukhin // Proceedings of the 11th International Conference "Pattern Recognition and Image Analysis: New Information Technologies" (PRIA-11-2013). - Samara, 2013. — P. 102–105.